Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2018 13 (6): 657-661

Multifactor Authentication - A Study on User Preference, Remembering Ability, Error Rate and Time Consumption

S. Vaithyasubramanian, D. Lalitha, M.I. Mary Metilda

Received 21 September 2018 ▪ Revised 29 October 2018 ▪ Accepted 30 November 2018

Abstract: In information security, the key element in course of action of identifying an individual based on their username and password is Authentication. In recent years, Information technology and security environment have been changing rapidly and dramatically. Various attack methods and vulnerabilities enforce service providers to look into alternate measures to enrich security process. To enhance security of the data web developers, service providers, professionals and researchers have developed different ways for users to authenticate in order to establish their access. Authentication approaches are poised to undergo some similar transformations in response. The system to address this challenge is by utilizing and integrating various existing authentication factors. Multifactor authentication is a technique comprises of the known validation process such as alphanumeric, graphical and biometric authentication. This process is easy to use, flexible and solid in authentications to expansive scale but requires memorability of passwords and time consuming. In this paper, study on user preference, remembering ability, error rate and time consumption of Multifactor authentication process is executed.

Keywords: Authentication, Password, Multifactor Authentication, Information Security.

INTRODUCTION

Looking into the future essentials in information security the authentication system needs to be designed in different way. To accomplish better security user needs to spend more to get progressively with additional measures of security. It is difficult, tough in trusting and preserving the security standards with time. With the evolution in computer technology only few challenges can be predictable, enhancement in cyber technology makes easier to various attack to Password database. Unwavering quality, comfort and protection of the information are the objectives of the security. This can be created by changing the authentication technique. To reduce the recurrences of wide-extending attacks and other online threats multi factor authentication is the alternate solution [1,4,5].

The standout amongst the best controls an service provider / user can actualize to keep an hacker from illegal accessing of network or a device to access the data is multifactor authentication. At the point when multifactor authentication is executed effectively, altogether it can make increasingly difficult for hackers to acquire authentic qualifications to encourage further malicious exercises on a system. Because of its competence, multifactor authentication is one of the Essential for effective security [8-11]. To an extensive scale multifactor authentication courses of action compose customers by adaptable and strong authentication. It requires memorability of authentication factors and in the same time easy to implement. In this paper, analysis on various key factors deciding towards the implementation of multifactor authentication is studied.

S. Vaithyasubramanian, Department of Mathematics, Sathyabama Institute of Science and Technology, Chennai, India. E-mail: discretevs@gmail.com

D. Lalitha, Department of Mathematics, Sathyabama Institute of Science and Technology, Chennai, India. E-mail: lalkrish2007@gmail.com

M.I. Mary Metilda, Department of Mathematics, Sathyabama Institute of Science and Technology, Chennai, India. E-mail: metilda81@gmail.com

REVIEW ON MULTIFACTOR AUTHENTICATION

Maria S. Millan et.al, (2006) demonstrated multifactor authentication by the combination of secret code and optical validation [2]. Steinberg and Joseph (2007) discussed the vulnerabilities of existing single factor authentication method. Further they addressed the weakness of security questions. As a solution to that they proposed two factor authentication [3]. Aloul F et.al, (2009) proposed two factor authentication method servicing transaction in ATM machines and online banking. It involves usage of mobile device at the time of transaction by implementing software token for OTP generation that too for user defined shorter time period. Implementation and testing of the suggested method has shown success concerning two factor authentication [6]. Nancie Gunson et.al, (2011) examined the study on user awareness of usability and security of existing and proposed method. In banking sector 62 customers were inspected for the comparative analysis. Single factor and two factor authentication approach were evaluated. Empherical analysis shows the significance difference between two methods and it justifies the evidence of practicing multifactor authentication for effective security [7]. Asoke Nath and Tanushree Mondal (2016) discussed the various aspects of security disputes in applying two factor authentication. With the rapid growth and development in information technology they suggest two factor and multi factor authentication as best security procedure [12]. Asif Amin et.al, (2017) discussed the significances of executing multifactor authentication. In their study they proposed a scheme of implementing computer based token as the second factor for validation [13]. Chenyu Wang et.al, (2018) studied the issues concerning the service provider in multiserver system. In their analysis they points out the problem of several attacks and non clarity in explanation of malicious entities which prevents users to reach their objective. To prevail over these flaws they proposed two factor authentication protocol for effective security [14]. Ometov A et.al, (2018) discussed the development of multifactor authentication from single factor authentication and various challenges of multifactor authentication [15].

Various studies shows that alternate to the existing single factor authentication is multifactor authentication to enhance efficient information security. Though multifactor authentication process is easy to implement but in execution various factors like remembering ability, system requirements and time consumptions are need to be analysed. In this paper, study on user preference, remembering ability, error rate and time consumption of Multifactor authentication process is executed.

RESULTS AND DISCUSSION

The present study has been analyzed towards user preference on multifactor authentication, remembering ability of authentication inputs and time taken by the users to input all three combination of authentication factors. Login authentication platform has been created and tested on 240 respondents. This study was an attempt to analyze the implementation process and to instruct users about the usage of multifactor authentication. A database was created and used to collect data for study. The database comprised of user name and user credentials. Study on user preference, user memory and time to enter the credentials were analyzed. The information obtained from the users were put through analysis and findings were represented graphically.

Analysis 1: User Preference

From the user study it is clear that 45% of the respondents favored two factor authentication, 35% preferred three factor authentication. The user preference is represented in figure 1. Preference concerning multi factor authentication may expand based on the users account category focusing effectual security. Also it is understandable that the user community are in need of alternate authentication process which emphasis more secure authentication procedures.

Figure 1: Respondents Preference towards multi factor Authentication

Analysis 2: Remembering Ability

One of the major issue associated with password is remembering ability. Even in single factor authentication long term memory tends user to create short and easily guessable alphanumeric passwords. Analysis shows that remembering ability will increase based on their usage, if users were asked to login regularly recollection of their password gets better. In the proposed authentication method they have to remember three authentication entry initially login id followed by something they know then something they click and finally something they have. For examination two factor authentication is contemplated the result is as shown in figure 2.

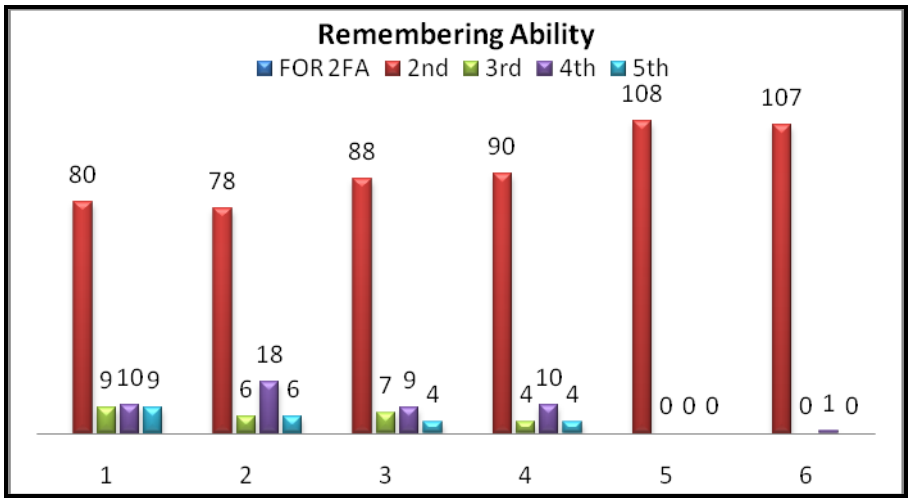

Figure 2: Remembering ability of MFA on various Attempts

Analysis 3: Error Rate

User were given five chances to recollect their authentication factor. The result and analysis shows the ability to remember the two factors for validations gets improved if they were frequently login their account. 86% of the users were able to execute their two authentication factor in the respective chances. 14% of error rate caused by the users to go for additional chances to complete their validation process is observed and represented in figure 3.

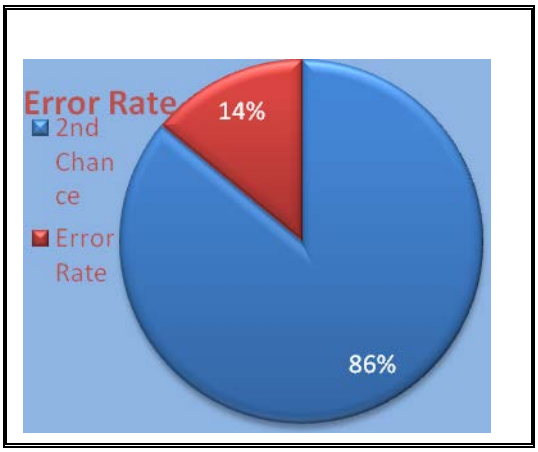

Figure 3: Error rate in implementation of Authentication type

Analysis 4: Time Consumption

In view of the fact that the proposed method is multi factor authentication the time complexity is one of the essential measure to be analyzed. Time to afford alphanumeric password, graphical password and biometric authentication of 50 users where examined. Without ignoring the incorrectness of the user input while affording the validation the analysis is performed. From the study it is clear that the time to execute all the three input for validation will increase and it is obvious. It takes an average of 15.9 and maximum of 25.5 seconds to afford all the three factor which is almost two times to enter alphanumeric password. It is understandable that multi factor authentication is time consuming process but extends the security features. Table 5 shows various basic measures of all types of validation process compared with three factor authentication.

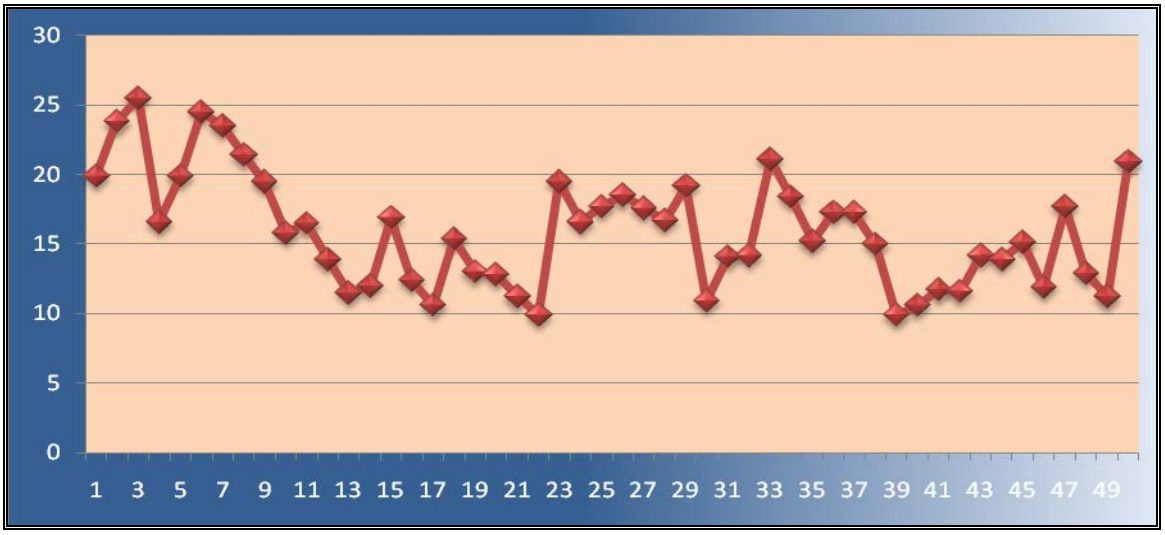

Figure 4: Time in seconds to afford all the three inputs for Authentication

Table 1: Various Measurements to enter Authentication

In Seconds	Alphanumeric	Graphical	Biometric	3FA
Average	7.55	4.6	3.8	15.9
Max	17.7	9.1	8	25.5
Min	2.1	2.9	1	9.9
Median	7.7	4.5	3.2	15.4

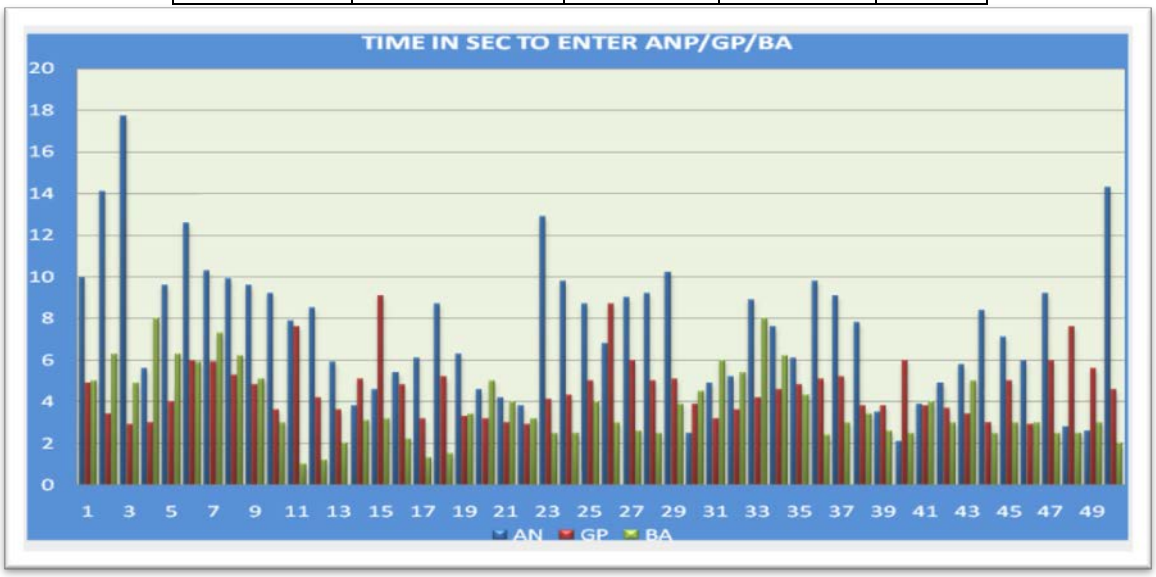

Figure 5: Time in seconds to enter three input for Authentication

CONCLUSION

To provide advanced alternatives to the existing method of validation, to overcome the threats and to improve the security of the authentication methods, the solution is multifactor authentication.

Multifactor authentication is often being used to work around the fundamental weaknesses in password management. While multifactor authentication does improve security, it increases user friction, a particular problem for online services that are not in a position to mandate multifactor authentication. Integrated multifactor authentication provides the best usability for better security. Multifactor authentication could definitely diminish the frequency of online extensive fraud and other online attacks. Analysis shows 45% and 35% of the respondents preferred two and three factor authentication respectively. This shows that user prefers multifactor authentication as it provides more security to the information. As a conclusion on this service providers or users can classify their login account as three categories and can implement single, two or three factor authentication. Study on remembering ability shows that initially users were unable to recall but as they were trying to re-login on repeated times /

days they were able to remember. It is clear and obvious that multifactor authentication consumes more time as the users has to implement all the verification factors.

REFERENCES

[1] Di Pietro R, Me G and Strangio M A (2005). “A two-factor mobile authentication scheme for secure financial transactions”, International Conference in Mobile Business, pp. 28-34.

[2] Maria S. Millan, Elisabet Perez-Cabre, and Bahram Javidi (2006) , "Multifactor authentication reinforces optical security," Opt. Lett. 31, 721-723.

[3] Steinberg, Joseph (2007). "System and method of using two or more multi-factor authentication mechanisms to authenticate online parties." U.S. Patent Application 11/606,788.

[4] Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. Journal of Computer Security, 15(5), 529-560.

[5] Sabzevar A P and Stavrou A (2008). “Universal multi-factor authentication using graphical passwords”, In Signal Image Technology and Internet Based Systems, pp. 625-632.

[6] Aloul, F., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on, 641-644. IEEE.

[7] Gunson, N, Marshall, D, Morton, H & Jack, M (2011). "User perceptions of security and usability of single factor and two-factor authentication in automated telephone banking" Computers & Security, vol. 30, no. 4, pp. 208-220. DOI: 10.1016/j.cose.2010.12.001.

[8] Mao Z, Florencio D and Herley C (2011). “Painless migration from passwords to two factor authentication”, In Information Forensics and Security, pp. 1-6.

[9] Adeoye O S (2012). “Evaluating the performance of two-factor authentication solution in the banking sector”, International Journal of Computer Science, Vol. 9, No.4, pp. 457-462.

[10] Singhal M and Tapaswi S (2012). “Software Tokens Based Two Factor Authentication Scheme”, International Journal of Information and Electronics Engineering, Vol. 2, No. 3, pp. 383.

[11] Dmitrienko A, Liebchen C, Rossow C and Sadeghi A R (2014). “On the security of mobile two-factor authentication”, In International Conference on Financial Cryptography and Data Security, pp. 365-383.

[12] Asoke Nath and Tanushree Mondal (2016). "Issues and Challenges in Two Factor Authentication Algorithms" International Journal of Latest Trends in Engineering and Technology, Vol. 6, Issue 3, 318 - 327.

[13] Asif Amin, Israr ul Haq, Monisa Nazir (2017, July). "Two factor Authentication" International Journal of Computer Science and Mobile Computing, Vol.6, Issue.7, 5-8.

[14] Wang, C., Xu, G., & Li, W. (2018). "A Secure and Anonymous Two-Factor Authentication Protocol in Multiserver Environment". Security and Communication Networks, Vol. 2018.

[15] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). "Multi-factor authentication: A survey". Cryptography, 2(1), 1.